The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
3/5/2012

SUBJECT:
Multiple Vulnerabilities in Adobe Flash Player Could Allow For Remote Code Execution (APSB12-05)

OVERVIEW:
Multiple vulnerabilities have been discovered in Adobe Flash Player that could allow attackers to take complete control of affected systems. Adobe Flash Player is a widely distributed multimedia and application player used to enhance the user experience when visiting web pages or reading email messages.

Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts will likely result in denial-of-service conditions.

SYSTEMS AFFECTED:
- Flash Player 11.1.102.62 and earlier for Windows, Macintosh, Linux and Solaris operating systems
- Flash Player 11.1.115.6 and earlier for Android 4.x
- Flash Player 11.1.111.6 and earlier for Android 3.x and 2.x

RISK:
Government:
Large and medium government entities: **High**
Small government entities: **High**
Businesses:
Large and medium business entities: **High**
Small business entities: **High**
Home users: High

DESCRIPTION:
Adobe Flash Player is prone to two unspecified vulnerabilities which could allow for remote code execution. Specific details for these vulnerabilities have not been released as of yet. There have been no reports of these vulnerabilities being exploited in the wild.

To exploit these vulnerabilities an attacker must create a specially crafted file or URL and distributes that file or URL to unsuspecting users via e-mail or some other means. When the file or URL is executed, the exploit occurs.

Successful exploitation of any of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts will likely result in denial-of-service conditions.

RECOMMENDATIONS:
The following actions should be taken:

- Install the updates provided by Adobe immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Do not open email attachments or click on URLs from unknown or untrusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails, IM (Instant Messages) or attachments especially from un-trusted sources.
- Consider implementing file extension whitelists for allowed e-mail attachments.

REFERENCES:

Adobe:
www.adobe.com/support/security/bulletins/apsb12-05.html

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0768
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0769

Security Focus:
http://www.securityfocus.com/bid/52297
http://www.securityfocus.com/bid/52299